Quelles obligations pour les OIV en matière de cybersécurité : exigences européennes et françaises comparées.

Par Betty Sfez, Avocat. - jeudi 17 avril 2014

Dans le cadre de sa stratégie européenne de lutte contre la cybercriminalité, la Commission européenne a adopté, en février 2013, une proposition de directive visant à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union. Ce texte vient d'être modifié et adopté en première lecture par le Parlement européen. [1]

Dernière mise à jour : 18 avril 2014

Cette proposition de directive repose sur un triple objectif : i) fixer des obligations aux États membres en matière de prévention et de gestion de risques et incidents touchant les réseaux et systèmes informatiques, ii) faciliter la coopération entre les États membres pour garantir l'harmonisation des règles de cybersécurité au sein de l'UE et, iii) établir des exigences en matière de sécurité pour "les acteurs du marché".

Ce texte précise notamment les obligations à la charge des "opérateurs d'infrastructure essentielle". Ces obligations sont en partie similaires à celles imposées aux opérateurs d'importance vitale (OIV) par la loi de programmation militaire française 2014-2019 (LPM 2014-2019) du 18 décembre 2013. [2] Nous proposons ci-dessous une synthèse des principales dispositions européennes en regard des nouvelles règles fixées par la LPM française.

1. Les acteurs concernés par les nouvelles dispositions

Toutes les entreprises ne sont pas concernées, ni par la future directive, ni par la LPM. La proposition de directive prévoit que seuls les "acteurs du marché" qualifiés d'opérateurs d'infrastructure essentielle, et dont l'effectif excède 10 personnes et le chiffre d'affaires annuel est supérieur à 2 millions d'euros, sont concernés par ces nouvelles obligations. Sont donc exclues les micro et petites entreprises, sauf exception. [3]

Ce texte rejoint les dispositions de la LPM 2014-2019, puisque les nouvelles obligations françaises en matière de cybersécurité concernent uniquement les opérateurs d'importance vitale. La notion française d'OIV est cependant plus large que la notion européenne d'opérateur d'infrastructure essentielle, dans la mesure où l'on ne distingue pas selon que l'OIV est une grande entreprise ou une PME, une société privée ou une administration publique. [4]

2. Les obligations de « cyber »sécurité

2.1 Détection et gestion des risques

La proposition de directive dispose que les organismes concernés doivent prendre des mesures préventives, d'ordre technique et organisationnel, visant à détecter et gérer les risques menaçant la sécurité de leurs réseaux et systèmes informatiques (RSI). Ces mesures doivent permettre d'éviter les incidents portant atteinte à la sécurité des RSI et réduire au minimum leur impact sur les services qu'ils fournissent.

Ces obligations sont à mettre en parallèle avec l'obligation de détection prescrite par la LPM 2014-2019. La loi française prévoit que dans certains cas, les OIV ont l'obligation de mettre en œuvre des systèmes qualifiés de détection des évènements susceptibles d'affecter la sécurité de leurs systèmes d'information. La procédure de qualification des outils de détection (sondes, etc.) et des prestataires proposant ce type de système doit être définie par décret.

2.2 Notification des incidents

Le projet de texte européen prévoit que les acteurs du marché doivent notifier à l'autorité compétente, sans retard injustifié, "les incidents qui ont impact significatif". Il s'agit d'incidents qui portent atteinte à la sécurité et à la continuité d'un réseau ou d'un système d'information et qui entraînent une perturbation notable de fonctions économiques ou sociétales essentielles.

Afin de déterminer l'ampleur de l'impact, trois critères à prendre en compte ont été proposés par le Parlement : le nombre d'utilisateurs dont le service essentiel est concerné, la durée de l'incident et la portée géographique eu égard à la zone touchée par l'incident.

Par ailleurs, la proposition de directive prévoit la possibilité, pour les autorités compétentes, d'informer le public d'un incident, si sa sensibilisation est nécessaire pour prévenir ou gérer un incident en cours, ou lorsque l'organisme concerné refuse de remédier à "une grave faiblesse structurelle sans délai injustifié". Les informations rendues publiques seront anonymes.

La LPM 2014-2019 prévoit également, à la charge des OIV, une obligation de déclarer sans délai au Premier ministre les incidents affectant le fonctionnement ou la sécurité de leurs SI. La loi ne définit pas la notion d'incident, qui doit être précisée par décret, ainsi que les modalités de la notification. En outre, la loi française ne prévoit pas expressément la possibilité pour l'Anssi ou les services de l'Etat d'informer le public en cas d'incident.

2.3 Mesures de sécurité et audit

La proposition de directive dispose que les autorités compétentes des États membres doivent être en mesure de veiller au respect des obligations par les acteurs du marché. Ces autorités doivent ainsi être dotées de pouvoirs leur permettant (i) de donner des instructions contraignantes, et (ii) d'exiger des acteurs du marché qu'ils fournissent des éléments prouvant la mise en œuvre effective des politiques de sécurité, tels que les résultats d'un audit réalisé par un organisme qualifié indépendant ou une autorité nationale.

La LPM 2014-2019 prévoit des obligations similaires. Les OIV doivent, d'une part respecter les règles et mesures de sécurité élaborées par le Premier ministre et, d'autre part soumettre leur SI à des audits destinés à vérifier le niveau de sécurité et le respect des règles de sécurité. Ces contrôles seront réalisés par des prestataires de service "qualifiés" ou les agents de l'Anssi.

3. Les sanctions en cas de non-respect des obligations

Le projet de texte européen précise que les Etats membres fixent eux-mêmes les sanctions applicables en cas de manquement aux obligations précitées. Il est intéressant de souligner que le texte amendé par le Parlement européen dispose que lorsque les acteurs du marché ne respectent pas les obligations, mais qu'ils n'ont pas agi de manière intentionnelle ou à la suite d'une négligence grave, aucune sanction ne doit être prononcée.

La LPM 2014-2019 sanctionne les manquements à la loi d'une amende de 150.000€, s'élevant à 750.000€ pour les personnes morales. La loi française ne distingue pas selon que le manquement est ou non intentionnel. La simple négligence est donc en principe condamnable.

La proposition de directive adoptée en première lecture par le Parlement doit maintenant être examinée par le Conseil. Si ce dernier accepte le texte tel quel, celui-ci sera définitivement adopté. A contrario, si le Conseil modifie le projet de texte, il sera renvoyé au Parlement en deuxième lecture. Dans un récent communiqué, Neelie Kroes, Vice-présidente de la Commission européenne, a précisé que les institutions européennes avaient émis le souhait que le projet final soit voté d'ici fin 2014.

Une fois la directive cybersécurité adoptée, elle sera en principe transposée, dans un délai de un an et demi, dans les différents droits nationaux. La France a pris les devants avec l'adoption de la loi de programmation militaire en décembre 2013 et la modification de son Code de la défense. Si les dispositions de la LPM 2014-2019 sont conformes aux orientations de politique européenne, la transposition du texte définitif de la directive est susceptible de nécessiter quelques aménagements en droit français.

A suivre donc …..

Betty SFEZ

Avocat au Barreau de Paris

Deleporte Wentz Avocat

http://www.deleporte-wentz-avocat.com/

Notes :

[1] Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, Bruxelles, le 7 février 2013. Voir à ce sujet notre article : http://dwavocat.blogspot.fr/2013/03 /cybersecurite-le-developpement-dune.html ; et Résolution législative du Parlement européen du 13 mars 2014 sur la proposition de directive NIS.

[2] Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

[3] Initialement, dans le projet de texte de la Commission, les nouvelles obligations incombaient aux administrations publiques et aux « acteurs du marché ». Les acteurs du marché étant définis et divisés en deux catégories :
- D'une part, « les prestataires de services de la société de l'information qui permettent la fourniture d'autres services de la société d'information », à savoir les : plateformes de e-commerce, réseaux sociaux, moteurs de recherches, services Cloud, etc.

- D'autre part, les « opérateurs d'infrastructure essentielle au maintien de fonctions économiques et sociétales vitales », dont la perturbation ou la destruction aurait une incidence considérable dans un État membre en conséquence du non-maintien de ces fonctions. Ces opérateurs exercent leurs activités dans les domaines de l'énergie (ex : gestionnaires de réseaux de distribution d'électricité), des transports (ex : transporteurs aériens), des services bancaires, des infrastructures de marchés financiers, des points d'échange internet, de la chaîne d'approvisionnement alimentaire et de la santé (ex : établissements de soins).

Par ailleurs, le texte initial excluait spécifiquement, les micro-entreprises et PME (effectif inférieur à 10 personnes et chiffre d'affaire annuel inférieur à 2 millions d'euros). En outre, bien que non expressément visé dans le texte, les députés avaient précisé que les développeurs de logiciels et les fabricants de matériel devaient être exclus du nouveau dispositif.

Enfin, voir article 14 §8 de la Résolution législative du 13 mars 2014 qui prévoit que les obligations précitées ne s'appliquent pas "aux micro-entreprises telles qu'elles sont définies dans la recommandation de la Commission 2003/361/CE du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, à moins que la micro-entreprise n'agisse comme succursale d'un acteur du marché".

[4] La réglementation portant sur les OIV figure aux articles L.1332-1 et s. du Code de la défense. Il s'agit d'opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement : (i) d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ; (ii) ou de mettre gravement en cause la santé ou la vie de la population.

Menu
Haut de page
Sommaire de la rubrique
Actualités Juridiques
Management
Emploi
Accueil du Village